EXHIBIT B

Patent Claims Analysis
of
US7523497 B2: "Packet flooding defense system"

against
Axway Amplify

US7523497B2

United States

Inventor Donald N. Cohen

Current Assignee Pacsec3 LLC

Worldwide applications

2000 US 2001 ~~WO~~ 2004 US

Application US10/841,064 events

2000-11-16	Priority to US09/715,813
2004-05-07	Application filed by Cohen Donald N
2004-11-18	Publication of US20040230839A1
2009-04-21	Application granted
2009-04-21	Publication of US7523497B2
2020-10-02	First worldwide family litigation filed
Status	Active
2022-11-05	Adjusted expiration

Owner name: PACSEC3 LLC, TEXAS

Free format text: ASSIGNMENT OF ASSIGNORS INTEREST;ASSIGNOR:COMPUTING SERVICES SUPPORT SOLUTIONS, INC.;REEL/FRAME:053526/0117

Effective date: 20200812

CLAIMS

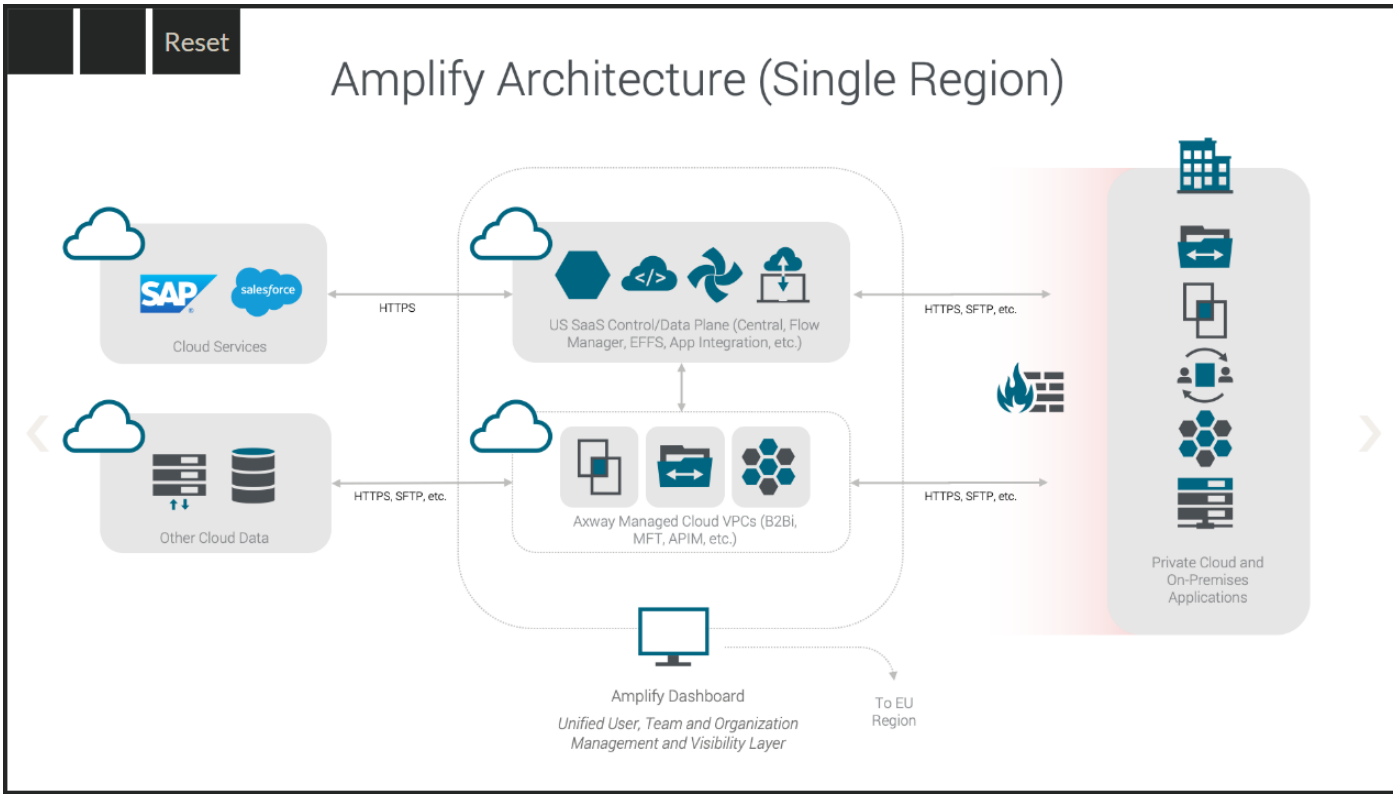
10. A method of providing packet flooding defense for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets, said method comprising the steps of:

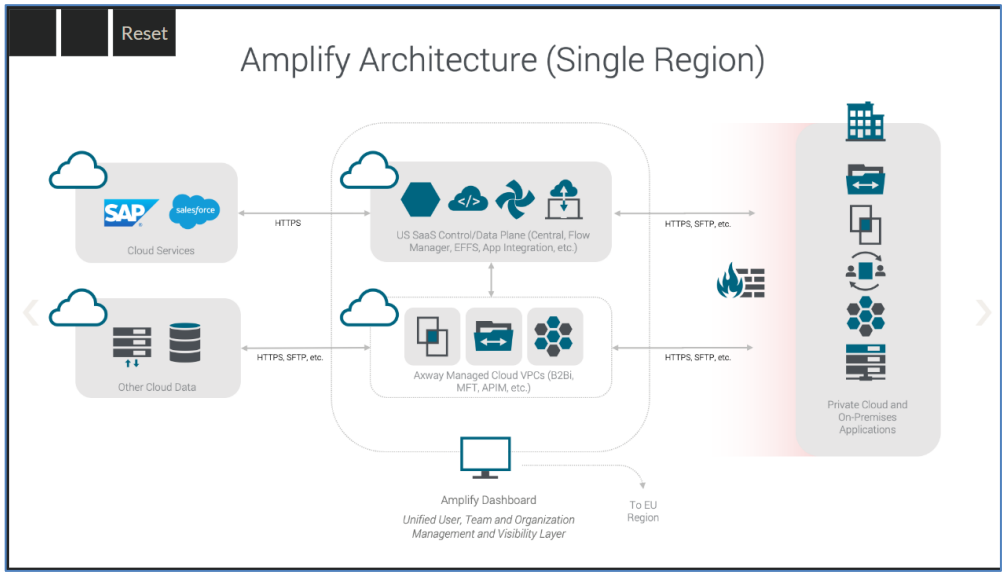
determining a path by which data packets arrive at said router via packet marks provided by routers leading to said host computer; said path comprising all routers in said network via which said packets are routed to said computer;

classifying data packets received at said router via packet marks provided by routers leading to said host computer by path;

associating a maximum acceptable transmission rate with each class of data packet received at said router; and

allocating a transmission rate equal to or less than said maximum acceptable transmission rate for unwanted data packets.

US7523497 B2 Claim 10	Axway Amplify
10. **A method of providing packet flooding defense for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets, said method comprising the steps of:**	 Axway Amplify has a packet flooding defense system for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets. https://docs.axway.com/bundle/axway_resources/page/amplify_api_management_platform_security_white_paper.html

US7523497 B2 Claim 10	Axway
determining a path by which data packets arrive at said router via packet marks provided by routers leading to said host computer; said path comprising all routers in said network via which said packets are routed to said computer;	Plaintiff contends that the managing of API traffic is "**controlled by Axway Control Access Lists and deployed in a protected DMZ**". "**Firewalls are placed in strategic choke points throughout the architecture of solutions**" and "**Each customer environment is deployed into individual Virtual Private Clouds, strictly segmented from other environments.**" "**For the Amplify SaaS platform, the DB has its own security group and own network segment. It does not receive any traffic outside the dedicated customer VPC.**" This means that Axway Amplify must have the ability to determine a path which packets arrive at a router leading to a host computer, because Axway states that "**Each customer environment is deployed into individual Virtual Private Clouds, strictly segmented from other environments.**"  *API Firewalling* All applications are installed behind an industry standard firewall, which are patched on a monthly basis. All access is controlled by Axway Control Access Lists and deployed in a protected DMZ. Firewalls are placed strategic choke points throughout the architecture of solutions. Each customer environment is deployed into individual Virtual Private Clouds, strictly segmented from other environments. For the Amplify SaaS platform, the DB has its own security group and own network segment. It does not receive any traffic outside the dedicated customer VPC. We have strict security rules which allow only nodes from the application cluster to make connections to the database. All DB nodes are part of different availability zones (AZ). All network devices are installed within a secure perimeter, physically accessible only to authorized personnel, and implemented with appropriate logical security. Where relevant to SaaS services deployed inside the Amplify cloud, there are very strict policies when it comes to interacting with customer data. Axway's underlying trusted cloud infrastructure providers keeps their "virtual endpoints and devices" separate from the customers infrastructure. https://docs.axway.com/bundle/axway_resources/page/amplify_api_management_platform_security_white_paper.html

US7523497 B2 Claim 10	Axway
classifying data packets received at said router via packet marks provided by routers leading to said host computer by path;	Plaintiff contends that once the **data packets arrive at the router** "**Gateway**", **the data packets are classified** "**The Gateway will detect and block threats**." This ensures that the router "**Gateway**" "**prevents attacks by inspecting the messages passing through it**." To protect the host computer (Data center). The Gateway prevents attacks by inspecting the messages passing through it. The Gateway provides API firewalling, content validation and message integrity checks which are in place to only allow legitimate messages to enter an organization. API Firewalling helps to mitigate against application-level threats, such as cross-site scripting, SQL injection, command injection, cross-site request forgery, etc. The Gateway will detect and block threats (i.e. OWASP top 10). Additionally, messages can be checked to see if they might contain viruses. Content validation is the ability to ensure that the request is appropriate for the requested API. The validation will check that the incoming request (and response) contains the appropriate parameters and values and that the payload adheres to the APIs schema. The Gateway will verify the integrity of the signed message (signed tokens, headers, payloads) to confirm that the message has not been tampered with in flight. In addition, it can ensure that some aspects of the payload remain confidential by encrypting, etc. The Gateway can act as an enforcement point which can delegate to a third-party system to make a decision on whether the message is good or bad (i.e., call ICAP server, PingIntelligence, etc.). The Gateway will enforce the decision from the third-party system. https://blog.axway.com/learning-center/digital-security/proxy-gateway/api-gateway-capabilities

US7523497 B2 Claim 10	Axway
associating a maximum acceptable transmission rate with each class of data packet received at said router; and	Plaintiff contends that once the data packets are classified into classes (wanted and unwanted data packets), a maximum acceptable transmission rate can be associated with each class of data packet. **"the Gateway sits in the line of traffic, it provides basic load balancing capabilities (Round Robin, Weighted Round Robin, random, etc.) for traffic entering the organization." "The Gateway provides various mechanisms for managing the rate of flow into an organization. It can protect your backend against severe traffic spikes and denial of service attacks."** This means that **"load balancing" will allow for the maximum acceptable transmission rate for wanted and unwanted data packets.** As the Gateway sits in the line of traffic, it provides basic load balancing capabilities (Round Robin, Weighted Round Robin, random, etc.) for traffic entering the organization. The Gateway provides various mechanisms for managing the rate of flow into an organization. It can protect your backend against severe traffic spikes and denial of service attacks. As it sits in the flow of traffic it can provide traffic throttling and smoothing. IP addresses can be white or blacklisted. Additionally, the Gateway provides various failure patterns, like a circuit breaker or retry policies, to help protect the organization from cascading failures. https://docs.axway.com/bundle/sync_datahub/page/configure_rate_limit_speed.html

US7523497 B2 Claim 10	Axway
allocating a transmission rate equal to or less than said maximum acceptable transmission rate for unwanted data packets.	Plaintiff contends that Axway will provide **a transmission rate** that is equal to or less than the maximum acceptable transmission rate, for example, a transmission rate of zero, meaning, "**block threats**". Or the system "**can provide traffic throttling**" to ensure the packets are inspected. As the Gateway sits in the line of traffic, it provides basic load balancing capabilities (Round Robin, Weighted Round Robin, random, etc.) for traffic entering the organization. The Gateway provides various mechanisms for managing the rate of flow into an organization. It can protect your backend against severe traffic spikes and denial of service attacks. As it sits in the flow of traffic it can provide traffic throttling and smoothing. IP addresses can be white or blacklisted. Additionally, the Gateway provides various failure patterns, like a circuit breaker or retry policies, to help protect the organization from cascading failures. The Gateway can act as an enforcement point which can delegate to a third-party system to make a decision on whether the message is good or bad (i.e., call ICAP server, PingIntelligence, etc.). The Gateway will enforce the decision from the third-party system. The Gateway prevents attacks by inspecting the messages passing through it. The Gateway provides API firewalling, content validation and message integrity checks which are in place to only allow legitimate messages to enter an organization. The Gateway will detect and block threats. https://docs.axway.com/bundle/sync_datahub/page/configure_rate_limit_speed.html